Continuous Diagnostics and Mitigation (CDM) Defect False Positive Triage Guide

15 April 2015

1 Purpose

The purpose of this document is to describe conditions that can cause a marked increase in the identification of defect false positives by a Continuous Diagnostics and Mitigation (CDM) capability collection system. A defect false positive condition occurs when a CDM capability collection system identifies a discrepancy between the actual state and the desired state and reports a defect when that defect is not actually present (e.g., an 'unauthorized device' defect is identified because an authorized device is not in the desired state but is operating on the network). When a false positive defect is reported, individuals and organizations that are assessed the risk of those defects are going to request that the risk points be removed from their score. The Department or Agency (D/A) is required to manage a process for receiving complaints about false positives as well as risk transfers, and will be referred to as the D/A grievance process for the purpose of this document. A large number of such complaints related to a particular defect imply some sort of systemic issue either in collection or analysis. This guide identifies the four generalized areas that can lead to systemic false positive identification for the Phase 1 CDM capabilities. It also includes triage tips for how to make a determination about the most likely error condition and assign the risk to the most appropriate role for resolution.

Often, the D/A grievance process will receive requests to transfer risks associated with reported defects from one role to another. An example of this is when devices have vulnerable software installed that cannot be patched due to a legacy application. When the administrator sees the vulnerable software defects, he or she can forward them to the D/A grievance process because they cannot mitigate the defect and the group that owns the application needs to be held accountable. In the case of false positives, no one else is identified as the person that should be held accountable, all that is known is that the person currently being held accountable has mitigated the defect or can prove that the defect does not exist. An example of this is when a particular software product that is mandatory is suddenly reported as not installed on a set of devices, but the administrator can verify that the software is installed.

Conditions that can lead to large numbers of false positive defects are related to problems with the following generalized areas:

- Desired state process related errors
- Misconfiguration or failures related to the collection system architecture, to include network design and inadequately or improperly deployed actual state sensors
- Incorrect actual state sensor types
- General data inconsistencies related to data integrity issues

Defects are reported to the base level dashboard (BLD) where they are prioritized to be corrected by the D/A administrators at the site. The administrators will identify situations they believe are not valid defects and pass those to the D/A grievance process. The D/A employees that participate in the grievance process can use this triage guide and the specific capability defect false positive guides to quickly identify the most likely false positive condition and then transfer the risk to the appropriate party for mitigation or investigation.

2 Roles and Responsibilities

To simplify this document, some basic roles are defined that should map to any D/A environment and CDM implementation. They are as follows:

Role	Responsiblities
Administrator	D/A employee or contractor support responsible for configuring and managing devices and systems. This role takes actions each day using the prioritized defect list in the CDM dashboard.
Desired State Manager (DSM)	Desired State Managers are needed for both the CDM Target Network and each device. The desired state managers ensure that data specifying the desired state of the relevant capability is entered into the CDM system's desired state data, and is available to guide the actual state collection sub-system.
Sensor Manager	D/A employee or the Continuous Monitoring as a Service (CMaaS) provider responsible for administering the actual state sensor.
Network Infrastructure Administrator	D/A employee or contractor support responsible for configuring and managing infrastructure devices.
Collection System Manager	D/A employee or CMaaS provider responsible for administering the actual or desired state collection system for the CDM capability.

The purpose of identifying applicable roles for different conditions is to help the D/A determine the role that will become the default for risk transfer and/or investigative actions to resolve issues presented to the grievance process as false positives.

As noted in supporting information throughout this document, certain conditions should produce alerts that are presented to certain roles. The D/A might want to make it standard operating policy that notice of these failures are provided to the grievance process to assist in assigning risk transfers to the party responsible for addressing the issue. Sometimes a spike in false positives will be the first indicator that a failure has occurred, and the D/A should establish a way for the grievance process to notify appropriate operations personnel of the potential issue. This can be done by the reassignment of the risk points to the associated role or some other form of communication.

3 False Positive Conditions

3.1. Desired State Process

The three main desired state process related issues that could lead to spikes in defect false positives are when desired state data is not synchronized, is inaccurate, or is incomplete.

Applicable roles: The Desired State Manager (DSM) for process related issues and the Collection System Manager for technology related issues.

Supporting Information: In most cases involving Desired State Process issues, the Administrator will likely recognize that there is a marked increase in the identification of a defect or set of defects for a set of devices or device types, that these defects did not exist previously for any of these devices, and that no changes had been performed in the operational environment related to those defects or devices.

Condition: *Synchronization* problems with the original data source (ODS)[1] can lead to spikes in defect false positives. Much of the time, this lack of synchronization will cause a single false positive, but there are some circumstances where defect false positive spikes can occur. An example of a defect false positive spike resulting from synchronization problems would be when a large number of changes are approved and/or made to the ODS and the operational environment, but these changes are not reflected in the desired state. This can occur when a major hardware upgrade is performed and all the new devices are not adequately listed in the desired state or are not associated with the previous devices listed in the desired state.

On occasion, a single change made to the ODS that is not reflected in the appropriate CDM desired state specification can cause a spike of false positives. A simple example of this is where a software products' license is renewed and the new expiration data is entered into the ODS but not into the associated desired state specification. When a Software Asset Management (SWAM) capability collection occurs after the expiration date in the desired state specification (but before the one in the ODS), then a false positive spike of "software product expired" will occur because the software product expiration defect will be identified for every device with the software product installed.

Condition: *Inaccuracies* in the desired state data can lead to spikes in defect false positives. Data inaccuracy issues can occur when desired state data becomes corrupted such as backup data or out-of-date restored backup data. This can occur when a legacy system is used to update the desired state and overwrites data that was previously corrected by the DSM.

Condition: *Incomplete* desired state data can also lead to spikes in defect false positives. This condition can occur when the information technology asset management (ITAM) tools, relied upon as desired state sensors, do not have current information available for all devices actively connected to the organization's network. It can also occur when the process for updating the CDM desired state specifications fails in some manner.

3.2. Architecture and Actual State Sensor Deployment

Architecture or actual state sensor deployment related issues that could lead to spikes in defect false positives are: infrastructure devices, actual state sensors, and/or the Actual State Collection Managers (ASCM) are misconfigured on the

[1] For many CDM capabilities, the D/A already has a set of tools and processes to officially document policy decisions. These are referred to as an Original Data Source (ODS) in this document. The information collected and maintained by the ODS is then "collected" and converted into desired state specifications by CDM technologies.

network; an element of the actual state collection system fails; the communication between two capabilities fails; or problems with the Data Store mechanism arise.

Applicable roles: Network Infrastructure Administrator for enterprise access control, routing, and connection issues; Sensor Manager for sensor issues; and the Collection System Manager for all other issues.

Condition: The network, actual state sensors, or ASCMs are *misconfigured* on the network such that the network security devices (e.g., firewalls) forbid either the collection of data by the sensors, the collection of data by the ASCM from the sensors, or the communication of data from the ASCMs to the actual state data repository. When this happens, there may be a spike in either non-reporting or other defects depending on implementation. For example, if the software inventory is not being collected from a device, there may be a spike in "Mandatory Software Not Installed" defects if the failure to collect is represented as an empty collection.

Supporting Information: This condition is most likely to occur during the "break in" period after initializing the CDM capability. It can also occur when the enterprise infrastructure is changed/upgraded, new actual state sensors are deployed, or the CDM collection capability is extended to include more devices.

Condition: There is a *failure* of an actual state sensor or an ASCM. An example of an actual state sensor failure is when a configuration checker fails in the *Configuration Settings Management* (CSM) capability resulting in the configuration checker incorrectly reporting 'not applicable' for a set of devices. This will create an increased number of failed CSM defect checks for those particular devices or a 'non-reporting' based on implementation. Both are considered a defect false positive because they are the result of the failed configuration checker and will be a spike because it affects all the devices the configuration checker is tasked to check.

Supporting Information: The Sensor Manager should be alerted when an actual state sensor fails and the Collection System Manager should be alerted if an instance of the ASCM fails.

Condition: There is a failure of the communication between two capabilities. For example, changes to installed software managed by the *Software Asset Management* (SWAM) capability doesn't get replicated to the CSM capability. Therefore, the CSM capability doesn't perform the required configuration checks resulting in an increase in false positive defects for the affected devices.

Supporting Information: The Collection System Manager should be alerted when data fails to transfer between CDM capabilities. If the transfer fails but there are no other failures associated with the sensors or ASCMs, then most likely network or security devices are preventing communications between the CDM capabilities.

Condition: There is a *failure* in a Data Store mechanism or of the capability to update the data store mechanism by one or more ASCMs, resulting in inaccuracies and/or synchronization issues with the actual state data. .

Supporting Information: The Collection System Manager should receive an alert showing that there is a problem with the collection system Data Store.

3.3. Incorrect Actual State Sensor Type

Sensor type issues that could lead to spikes in defect false positives are related to limitations on what data the sensor can see and report.

Applicable roles: The Collection System Manager is primarily responsible for selecting the correct actual state sensor type to deploy to properly collect actual state data elements for the CDM capability. The Sensor Manager is primarily responsible for configuration and operations of the sensor.

Supporting Information: This condition is most likely to occur during the "break in" period after initializing the CDM capability. It can also occur when new actual state sensors are deployed, existing actual state sensors are reconfigured, or the CDM collection capability is extended to include more devices.

Condition: An increased number of defect false positives can occur when an organization relies completely on the wrong actual sensor type or the correct sensor type is configured incorrectly. Deploying a wrong sensor type, just like misconfigurations of appropriate sensors, for data collection can lead to a defect false positive spike because it is either incapable of collecting the required data element or has limitations on what data it can see/sense. Subsequently, they will not provide data at the level of fidelity necessary to accurately identify defects.

Various actual state sensor types can be employed on the network that have differing or overlapping capabilities, and are usually placed within the network architecture to satisfy the needs of the network administrators rather than CDM needs. The sensor type selected is based on the type of data that is being targeted for collection. There are various sensor types that have their own unique capabilities and limitations and each sensor type must be carefully considered when determining sensor deployment and the data specifics required by the collection system. Refer to the 'Description of Actual State Sensor Types' document that applies to the particular capability to help determine if there are any known potential issues with using the selected sensor type.

In many cases the configuration or tuning of the deployed sensor will directly affect both the impact of the sensor on the network as well as the specific data that can be collected and the collection frequency. It is possible for changes that alleviate network concerns (i.e. bandwidth) to negatively impact the accuracy of the data collected for CDM purposes.

3.4. Data Integrity

Data issues that could lead to spikes in defect false positives are related to incompatible tool versions, misidentification, and format mismatches.

Applicable roles: Collection System Manager is responsible for identifying which hardware and software tools are authorized for the CDM capability. The Administrator or Sensor Manager employs the correct hardware or software tool to properly collect actual state data. The Collection System Manager, in coordination with the DSM, is responsible for resolving misidentified data elements and all data formatting issues.

Supporting Information: These conditions are most likely to occur during the "break in" period after initializing the CDM capability, especially when existing D/A specific tools are included in the deployment. They can also occur when new actual state sensors are deployed, existing actual state sensors are upgraded, or the CDM collection capability is extended to include more devices.

Condition: There are many hardware and software tools available to D/A's to use for collection of actual state data. The D/A's may want to use tools that are not part of the approved integrator's tool suite. Different tools may be used by the organization to collect the same type of actual state data from different operational environments. If the tool versions aren't properly documented and controlled, the tool version that was initially approved could be different from what is currently being utilized by the organization. Unmanaged version updates could result in changes in the tool functionality. All of these situations could affect how tools store, report, and collect data on objects resulting in inconsistent checks being implemented or incorrect algorithms being used to identify defects across tool sets. Different reporting formats and differing interpretation of data elements are areas of concern because data being combined and stored from various sources into a single database are highly

susceptible to changes in tools resulting in corrupt or inaccurate data. The nuances of how data from different sources is collected, reported, and integrated into existing actual state information can lead to spikes in capability defect false positives.

Condition: Actual state sensors could misidentify a device and include it in the actual state inventory, even when the device is not actually listed with the same identification data in the authorized hardware inventory. When an authorized device has incorrect identification data, this results in a mismatch between the actual state data and the desired state specification for the device.

Asset identities in a large-scale system are difficult to keep synchronized, and if a number of OSDs are used to initialize the desired state using ITAMs, then it is possible that they are inconsistent, resulting in desired state inconsistencies. The actual state information collected by the actual state sensors may deviate from the identifications used in the OSDs. This is most likely to occur during startup of a capability and cause false positive spikes of various kinds.

Supporting Information: The DSM will have to carefully review the identification schemes used and resolve data inconsistencies with the desired state. The Collection System Manager will have to ensure that actual state and desired state specification data are in formats that enable automated comparisons.

Condition: Data storage mechanisms could contain data formatting mismatches or structural issues with the actual state data. For example, tool vendors could intentionally obscure data due to intellectual property considerations. This can also be an issue if there are multiple actual state sensors collecting, storing, and reporting on the same data. Actual state sensors all have subtle nuances that differentiate them from each other (including sensors designed to collect the same type of information) and when combined, can cause abnormalities in the data it presents. Examples of actual state sensors not collecting the same data is when some sensors only collect a pass or fail state while others collect the value of the state when it did the check. When it comes to reporting on the same data and the nuances of sensors, an example of differences would be that some sensors will treat a ‘not applicable’ as a pass and others will treat it as not checked. This means careful consideration should be given to verify that a check was accomplished, the correct type of information was discovered, and how the information was reported back. This is especially true when dealing with pass or fail criteria and the assumptions that are made by the sensor.

Supporting Information: The Collection System Manager and Sensor Manager are responsible for problems related to collection system data storage. For this reason, a review and comparison of the data collected against the data that is displayed in storage should be accomplished.